UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/591,927	06/12/2000	Junichi Miura	16869P-008100	3690

20350 7590 07/19/2004

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 07/19/2004

9

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/591,927	MIURA ET AL.
	Examiner	Art Unit
	Christopher A. Revak	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-11,13-16,18-22,24,25,29,30 and 32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-11,13-16,18-22,24,25,29,30 and 32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-5,7-11,13-16,18-22,24, 25,29,30,32 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-5,7-11,13-16,18-22,24,25,29,30,32 are rejected under 35 U.S.C. 102(e) as being anticipated by Downs et al.

As per claim 1, Downs et al discloses of an electronic authentication method that generates an identifier that is associated with contents in a first information processing apparatus. The contents and identifier are combined to produce enhanced contents.

The enhanced content is transmitted to a second information processing apparatus. The enhanced content is presented to a user at the second information processing apparatus and the identifier is combined with the contents in a manner that is visually imperceptible to a user. User data is received in the second information processing apparatus to produce input data from the user data that includes obtaining the identifier from the enhanced content wherein user input data is produced based on the identifier. The input data is transmitted from the second information processing apparatus to the first information processing apparatus as received user input (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 2, Downs et al recites of generating a second identifier at the first information processing apparatus and storing the second identifier in a storage unit as a stored identifier. The second identifier is incorporates into the input data. Authentication occurs in the first information processing apparatus by comparing the input data and invalidating the stored identifier if the second identifier matches the stored input data (col. 10, lines 50-67 and col. 14, lines 19-28).

As per claim 3, it is taught by Downs et al of embedding an encryption key in the contents in the first information processing apparatus prior to transmission of the contents to the second information processing apparatus. User data is encrypted in the second information processing apparatus by using the encryption key prior to transmission of the input data to the first information processing apparatus. The

received input data is decrypted in the first information processing apparatus (col. 3, lines 42-55).

As per claim 4, Downs et al teaches that the embedded encryption key is a public key, the received input data is decrypted using a private key associated with the public key and the public key and private key are generated in the first information processing apparatus (col. 3, lines 42-51).

As per claim 5, Downs et al teaches of an information processing method that generates an identifier for contents, stores the identifier as a stored identifier, generates a second identifier, incorporates the identifier and second identifier with the contents to produce enhanced contents such that when the enhanced contents are displayed to a user, the identifier and second identifier is visually imperceptible. The enhanced contents are transmitted to and received by an external apparatus that acquires an identifier for the contents and carries out processing based on the received data and invalidates the stored identifier if the identifier matches the stored identifier (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 7, it is disclosed by Downs et al that the second identifier is an encryption key and receiving an identifier encrypted by using the encryption key and decrypting the received encrypted identifier (col. 3, lines 42-55).

As per claim 8, Downs et al teaches of an electronic authentication system comprising a first information processing apparatus and a second information processing apparatus. The first information processing apparatus generates an

identifier for contents, stores a first portion of the identifier as a stored identifier, transmits enhanced contents and the identifier to a second information processing apparatus that embeds the identifier in the contents to produce enhanced contents. The second information processing apparatus includes inputting user input data that includes displaying the received enhanced content such that the identifier is not visually perceivable by a user. User data is transmitted and the identifier for the first information processing apparatus is input data and the input data is generated by processing the user data and the first portion of the identifier based on a second portion of the identifier. The legitimacy of the input data is authenticated by the first information processing apparatus and invalidated the stored identifier if the first portion of the identifier contained in the input data matches the stored identifier (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 9, the teachings of Downs et al disclose a second information processing apparatus comprises an acquirement means for acquiring the identifier from the received enhanced contents (col. 25, lines 57-60 and col. 25, line 65 through col. 26, line 3).

As per claim 10, it is taught by Downs et al that the second portion of the identifier is an encryption key and the first information processing apparatus receives an identifier encrypted by using the encryption key and decrypting the encrypted identifier (col. 3, lines 42-55 col. 3, lines 42-55; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3).

As per claim 11, Downs et al teaches of an information processing apparatus that generates an identifier for contents, the identifier comprises a first part and a second part. The first part of the identifier is stored as a stored identifier. The contents and identifier are transmitted to an external apparatus as enhanced contents, wherein the enhanced contents include an identifier embedded in the contents such that upon displaying the enhanced contents to a user, the identifier is substantially visually imperceptible. The external apparatus receives data and acquires an identifier. The received data is processed and invalidated using the stored identifier if the acquired identifier matches the stored identifier (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 13, it is disclosed by Downs et al that the second portion of the identifier is an encryption key and an encrypted identifier is received by using an encryption key and decrypting the received encrypted identifier (col. 3, lines 42-55 col. 3, lines 42-55; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3).

As per claim 14, Downs et al teaches of an information processing apparatus that an external information processing apparatus to transmit content, receiving the requested content and an identifier embedded in the requested content, displaying the requested contents to a user such that the identifier is substantially visually imperceptible, extracting the identifier from the requested content, inputting user data from a user, and transmitting as secured data the user data and a first portion of the identifier to an external information processing apparatus, the secured data being

generated by using a second portion of the identifier (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 15, Downs et al recites that the second portion of the identifier in an encryption key and encrypts user data by using the encryption key (col. 3, lines 42-55 col. 3, lines 42-55; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3).

As per claim 16, Downs et al teaches of a storage medium for storing information readable by a computer that generates an identifier for contents, stores a first portion of the generated identifier, transmits the contents and the identifier to an external apparatus as enhanced contents such that upon displaying the enhanced contents to a user, the generated identifier is substantially visually imperceptible, receiving data from an external apparatus and acquiring an identifier from the contents for authenticating the legitimacy of the received data and invalidating the stored identifier if the acquired identifier matches the stored identifier (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 18, the teachings of Downs et al disclose that the generated identifier includes a second portion that is an encryption key that includes a function for receiving data encrypted by using an encryption key and decrypting the received encrypted data (col. 3, lines 42-55 col. 3, lines 42-55; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3).

As per claim 19, it is disclosed by Downs et al of a storage medium for storing information readable by a computer that includes a content requesting function for requesting an external information processing apparatus to transmit contents, receiving the requested contents and an identifier embedded in the contents, displaying the requested contents to a user wherein the identifier is substantially visually imperceptible, extracting the identifier from the contents, inputting user data, and transmitting the input data from the user and a first portion of the identifier to an external information processing apparatus, the input data is generated by using a second portion of the identifier (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 20, Downs et al recites that the second identifier is an encryption key and includes a function for encrypting user data by using an encryption key (col. 3, lines 42-55 col. 3, lines 42-55; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3).

As per claim 21, Downs et al teach of an electronic authentication method comprising generating an identifier for contents in a first information processing apparatus, the first information processing apparatus stores a first portion of the identifier and present time in a storage unit, transmitting the contents and identifier to a second information processing apparatus as enhanced content, wherein the identifier is embedded in the content, presenting the enhanced content to a user at the second information processing apparatus, the identifier being visually imperceptible to a user. User data is inputted from a user and is received by a second information processing

apparatus and transmitting the user data as secured data and the first portion of the identifier from the second information processing apparatus to the first information processing apparatus, the secure data being generated based on the second portion of the identifier. Invalidating the first portion of the identifier stored in the storage unit if the identifier received by the first information processing apparatus is not stored in the storage unit (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 22, Downs et al disclose of an electronic authentication method comprising generating an encryption key that is associated with contents in a first information processing apparatus, embedding the encryption key into the content to produce enhanced content such that when visible to a user, it is substantially imperceptible, transmitting the enhanced content to a second information processing apparatus, displaying the enhanced content in the second information processing apparatus, inputting user data that is received by the second information processing apparatus, encrypting user data using an encryption key to produce secured input data, including acquiring the encryption key from the enhanced content, transmitting the secured input data from the second information processing apparatus to the first information processing apparatus and validating the secured input data by decrypting the secured input data with a decryption key (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 24, Downs et al teaches of an authentication method in a system in which a first computer makes a request for a service is connected to a second computer rendering services via a network, request content being transmitted from the second computer to the first computer, data being transmitted from the first computer to the second computer associated with the contents. Generating at a second computer an access number for accessing the contents and cataloging the access number in a storage unit. Embedding the access number in the contents to produce enhanced content so that the access number is substantially visually imperceptible when the enhanced content is displayed and transmitting the enhanced content to the first computer. Displaying the content at the first computer and generating secured data at the first computer by processing user provided data with the access number fetched from the enhanced content and transmitting the secured data to the second computer. Authenticating the validity of the secured data by decrypting the secured data received at the second computer with a decryption key (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 25, it is taught by Downs et al that the encryption key is a public key and the decryption key is a private key (col. 3, lines 42-51).

As per claim 29, Downs et al disclose of a server apparatus comprising a processor, storage device, a network interface and bus for interconnecting the processor and storage device and network interface. The processor generates an encryption key for contents and transmits enhanced content comprising the content and

encryption key to an external apparatus via a network interface such that when the enhanced content is displayed, the encryption key is substantially visually imperceptible and the processor receives data from the external apparatus via the network interface, the data being encrypted with the encryption key (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

As per claim 30, it is disclosed by Downs et al that the encryption key is a public key component of a public key and private key encryption method (col. 3, lines 42-51).

As per claim 32, Downs et al teach of a client apparatus comprising a processor, input device, a network interface and bus interconnecting the processor, input device, and network interface. The processor requests an external information processing apparatus to transmit contents via a network interface, wherein the processor receives the content and encryption key embedded in the content, such that when the content is displayed to a user, the encryption key is substantially visually unperceivable and the processor extracts the encryption key from the contents, the processor receives user data from the input device and transmits the user data to the external information processing apparatus via the network interface by encrypting the user data with the encryption key (col. 3, lines 42-55; col. 10, lines 50-67; col. 14, lines 19-28; col. 25, lines 57-60; col. 25, line 65 through col. 26, line 3; col. 29, lines 29-61).

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 703-305-1843. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CR

July 7, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100